

CLAIMS

1. A method for securely storing information on a computer, said method comprising the steps of:
 - a) retrieving an identity of at least one computer component;
 - b) deriving at least one identifier from said identity of said at least one computer component; and
 - c) for each of said at least one identifier, storing said information on said computer in a storage entry corresponding to said identifier.
2. A method according to claim 1, wherein said deriving at least one identifier from said identity of said at least one computer component, is carried out in a secret manner.
3. A method according to claim 1, wherein said information is encrypted prior to said storing of said information.
4. A method according to claim 1, wherein said storage entry is selected from the group comprising: a file, a registry entry, a database entry.

5. A method according to claim 1, wherein said identity is selected from the group comprising: a serial number, a type number, a physical location, a network address.
6. A method according to claim 1, wherein said at least one computer component is selected from the group comprising: a hard drive, a network card, a CPU, a computer chip, a software element, a hardware element, a BIOS, a file, a name of a file, an ID of a file, a physical location of a file, a program.
7. A method according to claim 1, wherein said deriving of said at least one identifier from said identity of said at least one computer component is carried out by the steps:
 - a) generating a pseudo-random sequence whose seed is derived from said identity; and
 - b) deriving said at least one identifier from at least one member of said pseudo-random sequence.
8. A method according to claim 1, wherein said at least one computer component is remotely accessible by said computer.
9. A method according to claim 1, wherein said at least one storage entry is remotely accessible by said computer.

10. A method for securely storing information on a computer and retrieving said information, said method comprising the steps of:

storing said information by:

- a) retrieving an identity of at least one computer component;
- b) deriving at least one identifier from said identity of said at least one computer component;
- c) for each of said at least one identifier, storing said information on said computer in a storage entry corresponding to said identifier;

retrieving the stored information by:

- d) retrieving the identity of said at least one computer component;
- e) deriving in the manner of step (b) said at least one identifier from said identity of at least one computer component;
- f) for each of said at least one identifier, retrieving said information on said computer from a storage entry corresponding to said identifier;

11. A method according to claim 10, wherein said deriving at least one identifier from said identity of at least one computer component, is carried out in a secret manner.

12. A method according to claim 10, wherein said information is encrypted prior to said storing of said information.
13. A method according to claim 10, wherein said storage entry is selected from the group comprising: a file, a registry entry, a database entry.
14. A method according to claim 10, wherein said identity is selected from the group comprising: a serial number, a type number, a physical location, a network address.
15. A method according to claim 10, wherein said at least one computer component is selected from the group comprising: a hard drive, a network card, a CPU, a computer chip, a software element, a hardware element, a BIOS, a file, a name of a file, an ID of a file, a physical location of a file, a program.
16. A method according to claim 10, wherein said deriving of said at least one identifier from said identity of said at least one computer component is carried out by steps including:
 - a) generating a pseudo-random sequence whose seed is derived from said identity; and
 - b) deriving said at least one identifier from at least one member of said pseudo-random sequence.

17. A method according to claim 10, wherein said at least one computer component is remotely accessible by said computer.

18. A method according to claim 10, wherein said at least one storage entry is remotely accessible by said computer.